

1 Judge
2
3
4
5
6

Presented to the Court by the foreman of the
Grand Jury in open Court, in the presence of
the Grand Jury and FILED in the U.S.
DISTRICT COURT at Seattle, Washington.

4 *MARCH 3 2011*
5 WILLIAM M. MCCOOL, Clerk
6 By Deputy
7

7 UNITED STATES DISTRICT COURT
8 WESTERN DISTRICT OF WASHINGTON
9 AT SEATTLE

10 UNITED STATES OF AMERICA,

CR 11 NO 0070 RAJ

11 Plaintiff, } INDICTMENT

12 v.

(SEALED)

13 ROMAN SELEZNEV,
14 aka TRACK2,
15 aka ROMAN IVANOV,
16 aka RUBEN SAMVELICH,
17 aka nCuX,
18 aka Bulba,
aka bandysli64,
aka smaus,
aka Zagreb,
aka shmak.

19 Defendant.

20 The Grand Jury charges that:

21 COUNT 1

22 (Bank Fraud)

23 A. The Offense

24 1. Beginning at a time unknown, but no later than October 2, 2009, and
25 continuing through on or about January 20, 2011, within the Western District of
26 Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN
27 IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus,
28

1 aka Zagreb, aka shmak (hereinafter Roman Seleznev), and others unknown to the Grand
 2 Jury, knowingly and willfully devised and executed, and aided and abetted a scheme and
 3 artifice to defraud various financial institutions, including, but not limited, to Boeing
 4 Employees' Credit Union ("BECU"), Chase Bank, Capital One, Citibank, and Keybank
 5 ("the banks"), financial institutions as defined by Title 18, United States Code, Section
 6 20, and to obtain moneys, funds, and credits under the custody and control of the banks
 7 by means of material false and fraudulent pretenses, representations and promises, as
 8 further described below.

9 2. The object of the scheme and artifice to defraud was to "hack" into the
 10 computers of retail businesses within the Western District of Washington, and elsewhere;
 11 to install malicious computer code onto those hacked computers that would effectively
 12 steal the credit card numbers of the victim businesses' customers; to market and sell the
 13 stolen credit card numbers, on criminally inspired websites, for the purpose and with the
 14 intent that the stolen credit card numbers would then in turn be used for fraudulent
 15 transactions across the United States, and in foreign countries; and, by way of the scheme,
 16 to obtain illicit proceeds, funded by and derived primarily from the banks (located in the
 17 Western District of Washington, and elsewhere), that had originally issued the stolen
 18 credit card numbers. By way of this series of criminal actions, the defendants intended to
 19 and did generate and receive millions of dollars in illicit profits, that they then converted
 20 to their own personal benefit and use.

21 **B. Manner and Means of the Scheme and Artifice to Defraud**

22 3. ROMAN SELEZNEV has used "nics" or online nicknames in his dealings
 23 and his communications with others regarding and promoting the theft and sale of stolen
 24 credit card numbers that include: "TRACK2," "nCuX," "Bulba," "bandysli64," "smaus,"
 25 "Zagreb," and "shmak."

26 4. It was part of the scheme and artifice to defraud that ROMAN SELEZNEV,
 27 and others unknown to the Grand Jury, created a criminally inspired, Internet-based
 28

1 infrastructure to facilitate the theft, and then the sale, over the Internet, of credit card
2 account numbers that had been issued by banks, including BECU.

3 5. It was further part of the scheme and artifice to defraud that, as part of that
4 criminal Internet-based infrastructure, ROMAN SELEZNEV, and others unknown to the
5 Grand Jury, rented, configured, and controlled server computers in countries outside of
6 the United States, including the Ukraine and Russia, that contained malware, or malicious
7 computer code, which servers would provide downloads of that malware, onto other
8 computers, when the requesting computers were commanded to made such a request.

9 The server that hosted the malware was “named” “shmak.fvds.ru,” aka
10 “smaus.fvds.ru” aka “188.120.225.66” and all of the malware was located, on the server,
11 at shmak.fvds.ru/<malwarenamehere>. The server stored pieces of malware that been
12 denominated with names that included “shmak,” “shmak2,” “kameo,” “hameo” “zameo”
13 “dtc,” “dtc2,” “dtc4,” “dtca,” “rsca,” “remcomsvc,” and others. All of the malware was
14 located at the root of the server.

15 6. It was further part of the scheme and artifice to defraud that, as part of that
16 criminal Internet-based infrastructure, ROMAN SELEZNEV, and others unknown to the
17 Grand Jury, rented and configured server computers in countries outside of the United
18 States for the purpose of hosting carding forum websites, or websites used to sell stolen
19 credit card numbers, including carding forums named, “bulba.cc,” “secure.bulba.cc,”
20 “Track2.name” and “secure.Track2.name.”

21 7. It was further part of the scheme and artifice to defraud that, as part of that
22 criminal Internet-based infrastructure, ROMAN SELEZNEV, and others unknown to the
23 Grand Jury, rented and configured server computers, including servers in McLean,
24 Virginia, to receive and compile stolen credit card track data.

25 8. It was further part of the scheme and artifice to defraud that ROMAN
26 SELEZNEV, and others unknown to the Grand Jury, developed and used automated
27 techniques, such as port scanning, to identify computers and computer systems that were
28 connected to the Internet, that were dedicated to or involved with credit card processing

1 by retail businesses, and that would be vulnerable to criminal hacks for the purpose of
 2 stealing credit card numbers.

3 9. It was further part of the scheme and artifice to defraud that ROMAN
 4 SELEZNEV, and others unknown to the Grand Jury, used those automated techniques to
 5 identify credit card processing computers at the Broadway Grill restaurant, and at other
 6 businesses in the Western District of Washington as well as throughout the United States,
 7 as target computers for their criminal scheme.

8 10. It was further part of the scheme and artifice to defraud that once ROMAN
 9 SELEZNEV, and others unknown to the Grand Jury, identified credit card processing
 10 computers that were vulnerable to criminal hacks, they issued commands to the target
 11 computers to connect, over the Internet, to the servers that they had previously rented and
 12 configured and that they controlled, in the Ukraine and Russia, and to download malware
 13 from those servers, so that it would be installed on the victim target computers.

14 Specifically, once ROMAN SELEZNEV, and others unknown to the Grand Jury
 15 had remote control of a victim computer, they would launch a web browser on the victim
 16 computer. They would then type the address for the server hosting the malware
 17 (“shmak.fvds.ru,”) followed by the name of the piece of malware they wished to have
 18 downloaded (for example, “shmak.fvds.ru/kameo.exe”). The piece of malware specified
 19 could vary, as between the many different pieces of malware that were being hosted on
 20 the Ukraine/Russian server. Once this web address was typed into the address bar of the
 21 victim computer, the victim computer would download this piece of malware from the
 22 Ukraine/Russian server.

23 Once the malware was installed on the victim computer, ROMAN SELEZNEV,
 24 and others unknown to the Grand Jury, could disconnect from the victim computer. The
 25 malware that had been downloaded was preconfigured to upload credit card data that
 26 subsequently passed through the victim computer, to the server that had been designated
 27 by ROMAN SELEZNEV, and others unknown to the Grand Jury, for that purpose.
 28

1 In some cases ROMAN SELEZNEV, and others unknown to the Grand Jury, also
 2 installed a piece of software that would enable them to easily remotely reconnect to the
 3 victim servers again, at a later date.

4 11. It was further part of the scheme and artifice to defraud that the malware
 5 that ROMAN SELEZNEV, and others unknown to the Grand Jury caused to be installed
 6 on the targeted victim computers included software that monitored network activity
 7 within the business' internal computer network. The businesses that were targeted
 8 typically had several computers running, including a few "point of sale" terminals, and/or
 9 other computers that employees used to process orders, and to swipe customer credit
 10 cards when purchases were made. These computers were in turn connected to a
 11 computer, commonly referred to as the "the back of the house computer," or the
 12 "manager's computer," that would receive all of the credit card track data that had been
 13 gathered from the point of sale terminals; encrypt that data; and transmit it to the
 14 merchant card processor for approval.

15 The malware that ROMAN SELEZNEV, and others unknown to the Grand Jury
 16 caused to be downloaded to the victim business' computers monitored the traffic within
 17 the business' computer network and intercepted the communications between the point of
 18 sale terminals and the back of the house computer. The malware would extract and copy
 19 the data that included credit card track data and, every five minutes, compile the stolen
 20 credit card track data and transmit and upload it to a server identified by a specified IP
 21 address. That server had been previously rented and configured and was controlled by
 22 ROMAN SELEZNEV, and others unknown to the Grand Jury, for that purpose, and could
 23 be located in a variety of geographic locations, including in Russia, the Ukraine, or, for a
 24 time, in McLean, Virginia.

25 12. It was further part of the scheme and artifice to defraud that one of the
 26 business computer networks that was found vulnerable, and was hacked by ROMAN
 27 SELEZNEV, and others unknown to the Grand Jury, was that of the Broadway Grill
 28 restaurant, in Seattle, WA. In the case of the Broadway Grill, in particular, every credit

1 card number that had been swiped at the restaurant between December 1, 2009, and
 2 October 22, 2010, (over 32,000 unique credit card numbers) had been saved to a text file
 3 that was stored on the business' back of the house computer. ROMAN SELEZNEV, and
 4 others unknown to the Grand Jury, commanded the computer they hacked at the
 5 Broadway Grill restaurant to steal, transmit, and upload that complete text file, containing
 6 all of those unique credit card numbers, to computer servers specified by ROMAN
 7 SELEZNEV, and others unknown to the Grand Jury, that had previously been rented and
 8 configured and that were under their control, for that purpose.

9 ROMAN SELEZNEV, and others unknown to the Grand Jury, also caused and
 10 commanded the DTC2.exe malware to be installed on the manager's credit card
 11 processing computer at the Broadway Grill, in the manner described above, which
 12 malware then continued to steal any additional credit card track data, including credit card
 13 numbers, run after October 22, 2010. That data, as well, was transmitted from the
 14 infected Broadway Grill computer over the Internet, to computer servers specified,
 15 configured, and controlled by ROMAN SELEZNEV, and others unknown to the Grand
 16 Jury, for that purpose. The theft of credit card track data from Broadway Grill continued
 17 thereafter until the intrusion and theft were discovered on October 27, 2010.

18 13. It was further part of the scheme and artifice to defraud that, using the same
 19 techniques described above that were used to hack into, install malware, and steal credit
 20 card track data from the Broadway Grill restaurant in Seattle, WA, ROMAN
 21 SELEZNEV, and others unknown to the Grand Jury, hacked into, installed malware, and
 22 stole credit card tract data from a number of other small retail businesses in the Western
 23 District of Washington including, but not limited to: Grand Central Baking Company
 24 restaurant, in Seattle, WA; four Mad Pizza restaurants (three Seattle, WA, locations and a
 25 location in Tukwila, WA); Village Pizza, in Anacortes, WA, and Casa Mia Italian
 26 restaurant, in Yelm, WA.

27 14. It was further part of the scheme and artifice to defraud that, using the same
 28 techniques described above that were used to hack into, install malware, and steal credit

1 card track data from the Broadway Grill restaurant and other businesses in the Western
 2 District of Washington, ROMAN SELEZNEV, and others unknown to the Grand Jury
 3 likewise hacked into, installed malware, and stole credit card tract data from hundreds of
 4 retail businesses in other locations throughout the United States, including, but not limited
 5 to: Schlotzsky's Deli, in Coeur d'Alene, Idaho; Active Networks, in Frostburg, Maryland;
 6 Days Jewelry, in Waterville, Maine; Latitude Bar and Grill, in New York, New York;
 7 Grand Canyon Theatre, in Tusayan, Arizona; the Phoenix Zoo, in Phoenix, Arizona;
 8 Mary's Pizza Shack, in Sonoma, California; and City News Stand (a convenience store),
 9 at multiple store locations in Evanston, and Chicago, Illinois.

10 15. It was further part of the scheme and artifice to defraud that after credit card
 11 track data was transmitted from hacked businesses, and then compiled on the servers that
 12 ROMAN SELEZNEV, and others unknown to the Grand Jury had previously rented,
 13 configured, and controlled for that purpose, ROMAN SELEZNEV, and others unknown
 14 to the Grand Jury, harvested the data, and extracted and segregated from it credit card
 15 account numbers, Bank Identification Numbers ("BIN numbers,") and any other data
 16 possible, including names of the account holders or PIN numbers, that would enhance the
 17 value of the data for sale to those who wished to use it for criminal fraudulent purposes.

18 16. It was further part of the scheme and artifice to defraud that after ROMAN
 19 SELEZNEV, and others unknown to the Grand Jury, had stolen, harvested, and
 20 segregated the data that was valuable for sale to their would-be criminal customers, they
 21 then posted and marketed that data for sale on carding forum websites, including those
 22 named, "bulba.cc" and "Track2.name," which websites they had established on computer
 23 servers that they had rented, configured, and which they controlled, for this purpose. The
 24 stolen credit card numbers that they marketed and sold on these carding forum websites
 25 included credit card numbers that had been issued by BECU, and by other banks in the
 26 Western District of Washington and throughout the United States.

27 17. It was further part of the scheme and artifice to defraud that when ROMAN
 28 SELEZNEV, and others unknown to the Grand Jury advertised and sold stolen credit card

1 numbers, BIN numbers, and related stolen data for sale on their carding forum websites,
 2 they priced that data at varying levels, depending on its relative worth for use in
 3 fraudulent transactions. For example, credit card numbers with a “95%” guarantee for
 4 validity were priced between \$20 and \$30 per credit card track. This comprised the
 5 majority of the cards listed for sale. There were also credit card numbers listed at lower,
 6 “sale” prices. These were listed with a guarantee of validity of around “65%,” and were
 7 listed for sale at around \$7 per track.

8 18. It was further part of the scheme and artifice to defraud that ROMAN
 9 SELEZNEV, and others unknown to the Grand Jury would seek to attract and entice
 10 customers to their carding forum websites by advertising “fresh dumps” of stolen data,
 11 which included, for example, an advertisement on November 24, 2010, as follows:

12 UPDATE OF 38,000 USA (TRACK1+2) AND 5.000 USD
 13 TRACK2 ONLYTOTALLY MADE!!!
 14 90% VALID! BIG BASE, NEW60 - TRACK1+TRACK2,
 15 NEW61 - TRACK2 ONLY

16 And through an advertisement on December 23, 2010, as follows:

17 UPDATE 17,000 FRESH DUMPS TOTALY MADE! VALID
 18 VERY HIGH 95%!!
 19 75% TRACK1 + TRACK2 AND OTHER TRACK2 ONLY!!!
 20 Base - NEW65
 21 Warning - today checker not work at all. Sorry for that .
 22 Merry XMAS!(): THAT IS THE LAST UPDATE IN THIS YEAR. Hurry up to
 23 fund account

24 19. It was further part of the scheme and artifice to defraud that ROMAN
 25 SELEZNEV, and others unknown to the Grand Jury, sought to enhance the value and to
 26 spur sales of the stolen credit card data they marketed, for fraudulent use, by offering a
 27 “checker” service through the carding forum websites, which, for a fee, would enable
 28 customers to obtain instant validation information for the stolen credit card numbers, and

1 through which they also offered to "replace" numbers that were found to be invalid
2 through the checking service with an equal number of other stolen credit card numbers.

3 20. It was further part of the scheme and artifice to defraud that ROMAN
4 SELEZNEV, and others unknown to the Grand Jury, who controlled and operated the
5 bulba.cc and Track2.name carding forum websites, would only accept payment for the
6 stolen data that they sold through a limited number of payment services, including
7 webmoney services such as "Liberty Reserve," because those services hinder efforts to
8 trace the proceeds of the transactions and effectively conceal the identity of both the
9 payer and the recipients of the proceeds of the same.

10 21. It was further part of the scheme and artifice to defraud that, in order to
11 expand and maximize their customer base for stolen credit card numbers, ROMAN
12 SELEZNEV, and others unknown to the Grand Jury, advertised the carding forums that
13 they owned and controlled on other well known carding forum websites, such as
14 "crdsu.su" and "carder.biz."

15 22. It was further part of the scheme and artifice to defraud that, in order to
16 quash competition from other criminal carders, ROMAN SELEZNEV, and others
17 unknown to the Grand Jury, assumed total control and a monopoly over stolen credit card
18 sales made on the previously established and preeminent carder forum website named
19 "crdsu.su," in or around May of 2010.

20 23. It was further part of the scheme and artifice to defraud that ROMAN
21 SELEZNEV, and others unknown to the Grand Jury, stole over 200,000 credit card
22 numbers, and sold over 140,000 stolen credit card numbers through their carding forum
23 websites, bulba.cc and Track2.name, during the period from November 15, 2010, to
24 February 22, 2011.

25 24. It was further part of the scheme and artifice to defraud that ROMAN
26 SELEZNEV, and others unknown to the Grand Jury, generated illicit profits totaling at
27 least \$2,000,000.00 from the sale of stolen credit card information on the bulba.cc and
28 track2.name websites during the period from November 15, 2010, to February 22, 2011.

1 25. It was further part of the scheme and artifice to defraud that the stolen credit
 2 card numbers sold by ROMAN SELEZNEV, and others unknown to the Grand Jury, have
 3 been used to commit fraudulent transactions throughout the United States, including
 4 specifically in the States of Texas and New York, and throughout the world.

5 26. It was further part of the scheme and artifice to defraud that credit card
 6 numbers, in particular, that were stolen from the Broadway Grill by ROMAN
 7 SELEZNEV, and others unknown to the Grand Jury, which credit card numbers had been
 8 issued by BECU, were used in fraudulent transactions after their sale on the bulba.cc and
 9 track2.name websites for fraudulent transactions that have caused losses to BECU of at
 10 least \$79,317.00; and that credit card numbers stolen from Broadway Grill that were
 11 issued by other banks, and sold on the bulba.cc and Track2.name websites, have caused
 12 losses to the other banks that issued those cards in the amount of at least \$1,175,217.37.

13 **C. Execution of the Scheme and Artifice to Defraud**

14 27. On or about the below-listed dates, within the Western District of
 15 Washington and elsewhere, for the purpose of executing and attempting to execute this
 16 scheme and artifice to defraud, ROMAN SELEZNEV, and others unknown to the Grand
 17 Jury, did knowingly and willfully steal the credit card account numbers specified below,
 18 that had been issued by BECU, which account numbers subsequently were used in
 19 fraudulent transactions, causing a loss to BECU in the amounts specified below:

Count	Date CC # Stolen	CC Acct. Number Issued by BECU	BEAU Fraud Loss on Acct. No. Due to Fraudulent Transactions
1	10/22/2010	*****5719	\$1199.59
2	10/22/2010	*****6316	\$650.14
3	10/22/2010	*****7089	\$636.86
4	10/22/2010	*****0016	\$317.98
5	10/22/2010	*****0717	\$394.60

28 All in violation of Title 18, United States Code, Sections 1344 and 2.

COUNT 6

(Intentional Damage to a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On or about October 22, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly caused the transmission of a program, information, code, and command, and as a result of that conduct, intentionally caused and attempted to cause damage, without authorization, to a protected computer, to wit, by causing the installation of malware on credit card processing computer belonging to and located at the Broadway Grill restaurant, in Seattle, WA, and by such conduct caused loss to one or more persons during a one year period aggregating at least \$5,000 in value.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and 1030(c)(4)(B)(i), and 2.

COUNT 7

(Intentional Damage to a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On or about October 2, 2009, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly caused the transmission of a program, information, code, and command, and as a result of that conduct, intentionally caused and attempted to cause damage, without authorization, to a protected computer, to wit, by causing the installation of malware on the credit card processing computer belonging to and located at the Grand

1 Central Baking Company restaurant, in Seattle, WA, and by such conduct caused loss to
2 one or more persons during a one year period aggregating at least \$5,000 in value.

3 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and
4 1030(c)(4)(B)(i), and 2.

5

6 **COUNT 8**

7 **(Intentional Damage to a Protected Computer)**

8 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
9 fully set forth herein.

10 2. On our about August 28, 2010, within the Western District of Washington
11 and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka
12 RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb,
13 aka shmak, knowingly caused the transmission of a program, information, code, and
14 command, and as a result of that conduct, intentionally caused and attempted to cause
15 damage, without authorization, to a protected computer, to wit, by causing the installation
16 of malware on the credit card processing computer belonging to and located at the Mad
17 Pizza restaurant, in Tukwila, WA, and by such conduct caused loss to one or more
18 persons during a one year period aggregating at least \$5,000 in value.

19 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and
20 1030(c)(4)(B)(i), and 2.

21

22 **COUNT 9**

23 **(Intentional Damage to a Protected Computer)**

24 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
25 fully set forth herein.

26 2. On our about November 2, 2010, within the Western District of Washington
27 and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka
28 RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb,

1 aka shmak, knowingly caused the transmission of a program, information, code, and
2 command, and as a result of that conduct, intentionally caused and attempted to cause
3 damage, without authorization, to a protected computer, to wit, by causing the installation
4 of malware on the credit card processing computer belonging to and located at the Mad
5 Pizza restaurant, 1263 Thomas Street, Seattle, WA, and by such conduct caused loss to
6 one or more persons during a one year period aggregating at least \$5,000 in value.

7 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and
8 1030(c)(4)(B)(i), and 2.

9

10 **COUNT 10**

11 **(Intentional Damage to a Protected Computer)**

12 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
13 fully set forth herein.

14 2. On our about October 22, 2010, within the Western District of Washington
15 and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka
16 RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb,
17 aka shmak, knowingly caused the transmission of a program, information, code, and
18 command, and as a result of that conduct, intentionally caused and attempted to cause
19 damage, without authorization, to a protected computer, to wit, by causing the installation
20 of malware on the credit card processing computer belonging to and located at the Mad
21 Pizza restaurant, 1321 Madison St., Seattle, WA, and by such conduct caused loss to one
22 or more persons during a one year period aggregating at least \$5,000 in value.

23 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and
24 1030(c)(4)(B)(i), and 2.

1 **COUNT 11**

2 **(Intentional Damage to a Protected Computer)**

3 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
4 fully set forth herein.

5 2. On our about August 26, 2010, within the Western District of Washington
6 and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka
7 RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb,
8 aka shmak, knowingly caused the transmission of a program, information, code, and
9 command, and as a result of that conduct, intentionally caused and attempted to cause
10 damage, without authorization, to a protected computer, to wit, by causing the installation
11 of malware on the credit card processing computer belonging to and located at the Mad
12 Pizza restaurant, 4021 E. Madison St., Seattle, WA, and by such conduct caused loss to
13 one or more persons during a one year period aggregating at least \$5,000 in value.

14 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and
15 1030(c)(4)(B)(i), and 2.

16

17 **COUNT 12**

18 **(Intentional Damage to a Protected Computer)**

19 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
20 fully set forth herein.

21 2. On our about September 13, 2010, within the Western District of
22 Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN
23 IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus,
24 aka Zagreb, aka shmak, knowingly caused the transmission of a program, information,
25 code, and command, and as a result of that conduct, intentionally caused and attempted to
26 cause damage, without authorization, to a protected computer, to wit, by causing the
27 installation of malware the credit card processing computer belonging to and located at

1 the Village Pizza restaurant, in Anacortes, WA, and by such conduct caused loss to one or
2 more persons during a one year period aggregating at least \$5,000 in value.

3 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and
4 1030(c)(4)(B)(i), and 2.

5

6 **COUNT 13**

7 **(Intentional Damage to a Protected Computer)**

8 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
9 fully set forth herein.

10 2. On our about August 9 , 2010, within the Western District of Washington
11 and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka
12 RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb,
13 aka shmak, knowingly caused the transmission of a program, information, code, and
14 command, and as a result of that conduct, intentionally caused and attempted to cause
15 damage, without authorization, to a protected computer, to wit, by causing the installation
16 of malware on the credit card processing computer belonging to and located at the Casa
17 Mia Italian Pizzeria restaurant, in Yelm, WA, and by such conduct caused loss to one or
18 more persons during a one year period aggregating at least \$5,000 in value.

19 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and
20 1030(c)(4)(B)(i), and 2.

21

22 **COUNT 14**

23 **(Obtaining Information From a Protected Computer)**

24 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
25 fully set forth herein.

26 2. Beginning on a date uncertain, but on or about October 22, 2010, and
27 continuing until on or about October 27, 2010, within the Western District of Washington
28 and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka

1 RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb,
 2 aka shmak, intentionally accessed a computer without authorization, and thereby obtained
 3 information from a protected computer, to wit, they intentionally accessed the credit card
 4 processing computer belonging to and located at the Broadway Grill restaurant, in Seattle,
 5 WA, and obtained therefrom credit card track data that included credit card account
 6 numbers issued by Boeing Employees Credit Union or other financial institutions as
 7 defined by Title 18, United States Code, Section 20; and that they committed such offense
 8 in furtherance of a criminal and tortious act in violation of the Constitution and laws of
 9 the United States, specifically, bank fraud, in violation of Title 18, United States Code,
 10 Section 1344.

11 All in violation of Title 18, United States Code, Sections 1030(a)(2) and
 12 1030(c)(2)(B)(ii), and 2.

13

14 **COUNT 15**

15 **(Obtaining Information From a Protected Computer)**

16 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
 17 fully set forth herein.

18 2. Beginning on a date uncertain, but on or about October 2, 2009, and
 19 continuing until on or about December 1, 2010, within the Western District of
 20 Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN
 21 IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus,
 22 aka Zagreb, aka shmak, intentionally accessed a computer without authorization, and
 23 thereby obtained information from a protected computer, to wit, they intentionally
 24 accessed the credit card processing computer belonging to and located at the Grand
 25 Central Baking Company restaurant, in Seattle, WA, and obtained therefrom credit card
 26 track data that included credit card account numbers issued by Boeing Employees Credit
 27 Union or other financial institutions as defined by Title 18, United States Code, Section
 28 20; and that they committed such offense in furtherance of a criminal and tortious act in

1 violation of the Constitution and laws of the United States, specifically, bank fraud, in
2 violation of Title 18, United States Code, Section 1344.

3 All in violation of Title 18, United States Code, Sections 1030(a)(2) and
4 1030(c)(2)(B)(ii) and 2.

5

6 **COUNT 16**

7 **(Obtaining Information From a Protected Computer)**

8 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
9 fully set forth herein.

10 2. Beginning on a date uncertain, but on or about August 28, 2010, and
11 continuing until on or about February 1, 2011, within the Western District of Washington
12 and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka
13 RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb,
14 aka shmak, intentionally accessed a computer without authorization, and thereby obtained
15 information from a protected computer, to wit, they intentionally accessed the credit card
16 processing computer belonging to and located at the Mad Pizza restaurant, in Tukwila,
17 WA, and obtained therefrom credit card track data that included credit card account
18 numbers issued by Boeing Employees Credit Union or other financial institutions as
19 defined by Title 18, United States Code, Section 20; and that they committed such offense
20 in furtherance of a criminal and tortious act in violation of the Constitution and laws of
21 the United States, specifically, bank fraud, in violation of Title 18, United States Code,
22 Section 1344.

23 All in violation of Title 18, United States Code, Sections 1030(a)(2) and
24 1030(c)(2)(B)(ii) and 2.

COUNT 17

(Obtaining Information From a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. Beginning on a date uncertain, but on or about November 2, 2010, and continuing until on or about February 1, 2011, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, intentionally accessed a computer without authorization, and thereby obtained information from a protected computer, to wit, they intentionally accessed the credit card processing computer belonging to and located at the Mad Pizza restaurant, 1263 Thomas St., Seattle, WA, and obtained therefrom credit card track data that included credit card account numbers issued by Boeing Employees Credit Union or other financial institutions as defined by Title 18, United States Code, Section 20; and that they committed such offense in furtherance of a criminal and tortious act in violation of the Constitution and laws of the United States, specifically, bank fraud, in violation of Title 18, United States Code, Section 1344.

All in violation of Title 18, United States Code, Sections 1030(a)(2) and 1030(c)(2)(B)(ii) and 2.

COUNT 18

(Obtaining Information From a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. Beginning on a date uncertain, but on or about October 22, 2010, and continuing until on or about February 15, 2011, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus,

1 aka Zagreb, aka shmak, intentionally accessed a computer without authorization, and
2 thereby obtained information from a protected computer, to wit, they intentionally
3 accessed the credit card processing computer belonging to and located at the Mad Pizza
4 restaurant, 1321 Madison St., Seattle, WA, and obtained therefrom credit card track data
5 that included credit card account numbers issued by Boeing Employees Credit Union or
6 other financial institutions as defined by Title 18, United States Code, Section 20; and
7 that they committed such offense in furtherance of a criminal and tortious act in violation
8 of the Constitution and laws of the United States, specifically, bank fraud, in violation of
9 Title 18, United States Code, Section 1344.

10 All in violation of Title 18, United States Code, Sections 1030(a)(2) and
11 1030(c)(2)(B)(ii) and 2.

12

13 **COUNT 19**

14 **(Obtaining Information From a Protected Computer)**

15 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
16 fully set forth herein.

17 2. Beginning on a date uncertain, but on or about August 26, 2010, and
18 continuing until on or about February 15, 2011, within the Western District of
19 Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN
20 IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus,
21 aka Zagreb, aka shmak, intentionally accessed a computer without authorization, and
22 thereby obtained information from a protected computer, to wit, they intentionally
23 accessed the credit card processing computer belonging to and located at the Mad Pizza
24 restaurant, 4021 E. Madison St., Seattle, WA, and obtained therefrom credit card track
25 data that included credit card account numbers issued by Boeing Employees Credit Union
26 or other financial institutions as defined by Title 18, United States Code, Section 20; and
27 that they committed such offense in furtherance of a criminal and tortious act in violation

1 of the Constitution and laws of the United States, specifically, bank fraud, in violation of
2 Title 18, United States Code, Section 1344.

3 All in violation of Title 18, United States Code, Sections 1030(a)(2) and
4 1030(c)(2)(B)(ii) and 2.

5

6 **COUNT 20**

7 **(Obtaining Information From a Protected Computer)**

8 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
9 fully set forth herein.

10 2. Beginning on a date uncertain, but on or about September 25, 2010, and
11 continuing until on or about February 8, 2011, within the Western District of Washington
12 and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka
13 RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb,
14 aka shmak, intentionally accessed a computer without authorization, and thereby obtained
15 information from a protected computer, to wit, they intentionally accessed the credit card
16 processing computer belonging to and located at the Village Pizza restaurant, Anacortes,
17 WA, and obtained therefrom credit card track data that included credit card account
18 numbers issued by Boeing Employees Credit Union or other financial institutions as
19 defined by Title 18, United States Code, Section 20; and that they committed such offense
20 in furtherance of a criminal and tortious act in violation of the Constitution and laws of
21 the United States, specifically, bank fraud, in violation of Title 18, United States Code,
22 Section 1344.

23 All in violation of Title 18, United States Code, Sections 1030(a)(2) and
24 1030(c)(2)(B)(ii) and 2.

1 **COUNT 21**

2 **(Obtaining Information From a Protected Computer)**

3 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
4 fully set forth herein.

5 2. Beginning on a date uncertain, but on or about August 9, 2010, and
6 continuing until on or about February 23, 2011, within the Western District of
7 Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN
8 IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus,
9 aka Zagreb, aka shmak, intentionally accessed a computer without authorization, and
10 thereby obtained information from a protected computer, to wit, they intentionally
11 accessed the credit card processing computer belonging to and located at the Casa Mia
12 Italian Pizzeria restaurant, Yelm, WA, and obtained therefrom credit card track data that
13 included credit card account numbers issued by Boeing Employees Credit Union or other
14 financial institutions as defined by Title 18, United States Code, Section 20; and that they
15 committed such offense in furtherance of a criminal and tortious act in violation of the
16 Constitution and laws of the United States, specifically, bank fraud, in violation of Title
17 18, United States Code, Section 1344.

18 All in violation of Title 18, United States Code, Sections 1030(a)(2) and
19 1030(c)(2)(B)(ii) and 2.

20 **COUNT 22**

21 **(Possession of Fifteen or More Unauthorized Access Devices)**

22 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
23 fully set forth herein.

24 2. On or about January 20, 2011, within the Western District of Washington
25 and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka
26 RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb,
27 aka shmak, knowingly and with intent to defraud, possessed fifteen or more unauthorized
28

1 access devices, that is, credit card account numbers that belonged to individuals who were
 2 customers of businesses located within the Western District of Washington, which credit
 3 card account numbers ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka
 4 RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb,
 5 aka shmak, stole from businesses, including the Broadway Grill, the Grand Central
 6 Baking Company, several Mad Pizza restaurants, Village Pizza, and Casa Mia Italian
 7 Pizzeria, located in the Western District of Washington, said possession affecting
 8 interstate and foreign commerce, in that the unauthorized access devices were possessed
 9 in order to market and sell them to others, for the intended purpose of making fraudulent
 10 purchases in multiple states within the United States, and foreign countries.

11 All in violation of Title 18, United States Code, Sections 1029(a)(3) and
 12 1029(c)(1)(A)(i), and 2.

13

14 **COUNT 23**

15 **(Trafficking in Unauthorized Access Devices)**

16 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
 17 fully set forth herein.

18 2. From on or about November 15, 2010, to on or about November 16, 2010,
 19 within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka
 20 TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba,
 21 aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly and with intent to defraud,
 22 trafficked in credit card track data, including credit card account numbers for credit card
 23 accounts that were established through and issued by the Boeing Employees Credit
 24 Union, in the Western District of Washington, and by such conduct, from on or about
 25 November 15, 2010, and ending on or about November 16, 2010, obtained profits
 26 aggregating approximately \$83,490.00, said trafficking affecting interstate and foreign
 27 commerce, in that the credit card account numbers that were so trafficked were in turn

1 used to make fraudulent purchases in multiple states within the United States, and foreign
2 countries.

3 All in violation of Title 18, United States Code, Sections 1029(a)(2) and
4 1029(c)(1)(A)(i), and 2.

5

6 **COUNT 24**

7 **(Trafficking in Unauthorized Access Devices)**

8 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
9 fully set forth herein.

10 2. From on or about January 31, 2011, to on or about February 1, 2011, within
11 the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2,
12 aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka
13 bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly and with intent to defraud,
14 trafficked in credit card track data, including credit card account numbers for credit card
15 accounts that were established through and issued by the Boeing Employees Credit
16 Union, in the Western District of Washington, and by such conduct, from on or about
17 January 31, 2011, and ending on or about February 1, 2011, obtained profits aggregating
18 approximately \$30,716.00, said trafficking affecting interstate and foreign commerce, in
19 that the credit card account numbers that were so trafficked were in turn used to make
20 fraudulent purchases in multiple states within the United States, and foreign countries.

21 All in violation of Title 18, United States Code, Sections 1029(a)(2) and
22 1029(c)(1)(A)(i), and 2.

23

24

25

26

27

28

COUNT 25

(Aggravated Identity Theft)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On or about October 22, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly transferred, possessed and used, without lawful authority, a means of identification of another person, to wit, the personally identifiable credit card number of ****-****-****-5719, belonging to D.K., of Seattle, WA, within the Western District of Washington, during and in relation to a felony listed in Title 18, United States Code, Section 1028A(c), to wit, Bank Fraud, in violation of Title 18, United States Code, Section 1344.

All in violation of Title 18, United States Code, Sections 1028(a)(1) and 2.

COUNT 26

(Aggravated Identity Theft)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On or about October 22, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly transferred, possessed and used, without lawful authority, a means of identification of another person, to wit, the personally identifiable credit card number of ****-****-****-7089, belonging to N.S., of Seattle, WA, within the Western District of Washington, during and in relation to a felony listed in Title 18, United States Code,

1 Section 1028A(c), to wit, Bank Fraud, in violation of Title 18, United States Code,
2 Section 1344.

3 All in violation of Title 18, United States Code, Sections 1028(a)(1) and 2.

4

5 **COUNT 27**

6 **(Aggravated Identity Theft)**

7 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
8 fully set forth herein.

9 2. On or about October 22, 2010, within the Western District of Washington
10 and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka
11 RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb,
12 aka shmak, knowingly transferred, possessed and used, without lawful authority, a means
13 of identification of another person, to wit, the personally identifiable credit card number
14 of ****-****-****-0016, belonging to T.A., of Seattle, WA, within the Western District
15 of Washington, during and in relation to a felony listed in Title 18, United States Code,
16 Section 1028A(c), to wit, Bank Fraud, in violation of Title 18, United States Code,
17 Section 1344.

18 All in violation of Title 18, United States Code, Sections 1028(a)(1) and 2.

19

20 **COUNT 28**

21 **(Aggravated Identity Theft)**

22 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
23 fully set forth herein.

24 2. On or about October 22, 2010, within the Western District of Washington
25 and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka
26 RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb,
27 aka shmak, knowingly transferred, possessed and used, without lawful authority, a means
28 of identification of another person, to wit, the personally identifiable credit card number

1 of ****-****-****-0717, belonging to J.H., of Seattle, WA, within the Western District
2 of Washington, during and in relation to a felony listed in Title 18, United States Code,
3 Section 1028A(c), to wit, Bank Fraud, in violation of Title 18, United States Code,
4 Section 1344.

5 All in violation of Title 18, United States Code, Sections 1028(a)(1), and 2.
6

7 **COUNT 29**

8 **(Aggravated Identity Theft)**

9 1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if
10 fully set forth herein.

11 2. On or about October 22, 2010, within the Western District of Washington
12 and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka
13 RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb,
14 aka shmak, knowingly transferred, possessed and used, without lawful authority, a means
15 of identification of another person, to wit, the personally identifiable credit card number
16 of ****-****-****-6316, belonging to L.S., of Seattle, WA, within the Western District
17 of Washington, during and in relation to a felony listed in Title 18, United States Code,
18 //
19 //
20 //
21 //
22 //
23 //
24 //
25 //
26 //
27 //
28 //

1 Section 1028A(c), to wit, Bank Fraud, in violation of Title 18, United States Code,
2 Section 1344.

3 All in violation of Title 18, United States Code, Sections 1028(a)(1), and 2.

4

5

A TRUE BILL:

6

DATED:

7

8

Signature of the Foreperson redacted pursuant
to the policy of the Judicial Conference

9

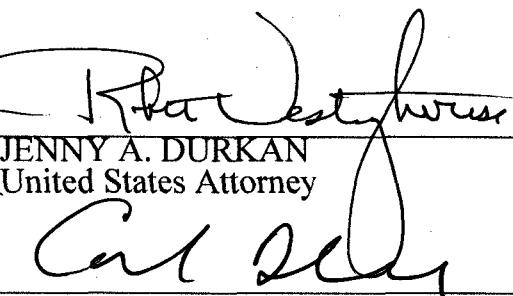
_____ FOREPERSON

10

11

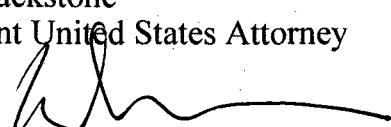
JENNY A. DURKAN
United States Attorney

12


Carl Blackstone
Assistant United States Attorney

13

14


Kathryn A. Warma
Assistant United States Attorney

15

16

17

18

19

20

21

22

23

24

25

26

27

28

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970